This listing of claims will replace all prior versions, and listings, of claims in the application:

IN THE CLAIMS:

1. (Currently Amended) A method of transmitting data securely over a computer network, comprising the steps of:

(1) establishing a communication path between a first computer and a second computer;

(2) encrypting and transmitting data records between the first computer and the second computer using an unreliable communication protocol, wherein each data record incorporates a nonce and encrypted text that has been ~~a nonce and is~~ encrypted using the nonce without reference to a previously transmitted data record; and

(3) in the second computer, receiving and decrypting the data records transmitted in step (2) by, for each of the received data records, decrypting the incorporated encrypted text ~~by~~ using the incorporated nonce in combination with a previously shared encryption key ~~to decrypt each of the data records~~ without reference to a previously received data record.

2. (Original) The method of claim 1, further comprising the step of, prior to step (1), establishing a reliable communication path between the first computer and the second computer and exchanging security credentials over the reliable communication path.

3. (Original) The method of claim 2, wherein the step of exchanging security credentials comprises the step of exchanging an encryption key that is used to encrypt the data records in step (2).

4. (Canceled)

5. (Previously Presented) The method of claim 1, wherein the nonce comprises a random number.

6. (Currently Amended) The method of claim 1, further comprising the step of, in the

second computer, verifying for each received data record that the incorporated nonce has not previously been received in a previously transmitted data record.

7. (Currently Amended) The method of claim 1,

wherein step (2) comprises the step of embedding an indicator in each of the encrypted data records indicating that the encrypted data records incorporate encrypted text that has been ~~are~~ encrypted according to an encryption scheme that encrypts ~~records~~ text without regard to any previously transmitted data records, and

wherein step (3) comprises the step of determining whether the indicator is present in each received record and, in response to determining that the indicator is not present, processing each such record differently than if the indicator is set.

8. (Original) The method of claim 1, wherein step (1) is performed using the Transmission Control Protocol, and wherein step (2) is performed using the User Datagram Protocol.

9. (Original) The method of claim 1, wherein step (2) is performed by a proxy server that encrypts data records received from another server.

10. (Currently Amended) A method of securely transmitting a plurality of data records between a client computer and a proxy server using an unreliable communication protocol, comprising the steps of:

(1) establishing a reliable connection between the client computer and the proxy server;

(2) exchanging encryption credentials between the client computer and the proxy server over the reliable connection;

(3) generating a nonce for each of a plurality of data records, wherein each nonce comprises an initialization vector necessary to encrypt text for ~~decrypt~~ a corresponding one of the

plurality of data records;

(4) for each of the plurality of data records, using the corresponding nonce to encrypt ~~each of the plurality of data records~~ text and incorporating the encrypted text and the corresponding ~~and appending the~~ nonce into the ~~to each of the plurality of~~ data record ~~records~~;

(5) transmitting the plurality of data records encrypted in step (4) from the client computer to the proxy server using an unreliable communication protocol; and

(6) in the proxy server, decrypting the encrypted text in each of the plurality of encrypted data records using the a corresponding nonce extracted from each data record and a previously shared encryption key.

11. (Original) The method of claim 10, wherein step (6) comprises the step of checking to determine whether each data record received from the client computer is formatted according to a secure unreliable transmission format and, if a particular record is not formatted according to a secure unreliable transmission format, bypassing the decryption using the corresponding nonce.

12. (Original) The method of claim 10, wherein step (3) comprises the step of generating a random number as each nonce.

13. (Original) The method of claim 10, wherein step (1) is performed using Transmission Control Protocol, and wherein step (5) is performed using User Datagram Protocol.

14. (Original) The method of claim 10, wherein step (6) is performed using an encryption key previously shared using a reliable communication protocol.

15. (Original) The method of claim 14, wherein the reliable communication protocol is Transmission Control Protocol.

16. (Currently Amended) A system for securely transmitting data using an unreliable protocol, comprising:

a first computer comprising a communication protocol client function operable in conjunction with an application program to transmit data records securely using an unreliable protocol; and

a second computer coupled to the first computer and comprising a communication protocol server function operable in conjunction with the communication protocol client function to receive data records securely using the unreliable communication protocol,

wherein, for each data record, the communication protocol client function encrypts text for the ~~each~~ data record using a nonce and an encryption key and ~~appends~~ incorporates the respective encrypted text and nonce in the ~~to each of the encrypted~~ data record ~~records~~; and

wherein the communication protocol server function decrypts the encrypted text in each of the data records using the respectively appended nonce and the encryption key.

17. (Original) The system of claim 16, wherein the communication protocol client function exchanges encryption credentials with the communication protocol server function using a reliable communication protocol.

18. (Original) The system of claim 17, wherein the unreliable communication protocol comprises the User Datagram Protocol, and wherein the reliable communication protocol comprises the Transmission Control Protocol.

19. (Original) The system of claim 16, wherein the communication protocol client function and the communication protocol server function are compatible with the SOCKS communication protocol.

20. (Original) The system of claim 16, wherein the communication protocol client function and the communication protocol server function are compatible with the SSL/TLS communication protocol.

21. (Currently Amended) The system of claim 16, wherein the second computer comprises a proxy server that forwards the decrypted text ~~records received from the first computer~~ to a server computer.

22. (Original) The system of claim 16, wherein the second computer comprises a record detector that determines whether an indicator has been set in each data record received from the first computer and, if the indicator has not been set, bypassing decryption in the server computer.

23. (Currently Amended) A method of transmitting data securely over a computer network, comprising:

establishing a communication path with a remote computer;

encrypting data records using a nonce such that each data record incorporates

~~a~~ the nonce, and

text that is encrypted such that the remote computer can decrypt the encrypted text ~~each of the data records~~ by using the incorporated nonce in combination with a previously shared encryption key and without reference to a previously received data record; and

transmitting the encrypted data records to the remote computer using an unreliable communication protocol.

24. (Previously Presented) The method of claim 23, further comprising establishing a reliable communication path to the remote computer and exchanging security credentials with the remote computer over the reliable communication path.

25. (Currently Amended) The method of claim 24, wherein the step of exchanging security credentials includes exchanging an encryption key that is used to encrypt the text ~~data records~~.

26. (Previously Presented) The method of claim 23, wherein the nonce includes a random

number.

27. (Currently Amended) The method of claim 23, wherein encrypting the data records includes embedding an indicator in each of the data records indicating that the ~~data records are~~ record incorporates text encrypted according to an encryption scheme that encrypts ~~records~~ text without regard to any previously transmitted data records, such that the remote computer can determine whether the indicator is present in each received data record and, in response to determining that the indicator is not present, process each such received data record differently than if the indicator is set.

28. (Previously Presented) The method of claim 23, wherein

establishing the communication path with the remote computer is performed using the Transmission Control Protocol, and

encrypting the data records is performed using the User Datagram Protocol.

29. (Currently Amended) The method of claim 23, wherein encrypting the data records is performed by a proxy server that encrypts ~~data records~~text received from another server.

30. (Currently Amended) A method of transmitting data securely over a computer network, comprising:

establishing a communication path with a remote computer;

receiving data records

transmitted from the remote computer using an unreliable communication protocol, and

encrypted using a nonce such that

~~each data record incorporates a nonce and~~

text that is encrypted without reference to a previously encrypted data

record ; and

decrypting the received data records by using the nonce in combination with a previously shared encryption key to decrypt each received data record without reference to a previously received data record.

31. (Previously Presented) The method of claim 30, further comprising establishing a reliable communication path with the remote computer and exchanging security credentials with the remote computer over the reliable communication path.

32. (Previously Presented) The method of claim 31, wherein exchanging security credentials includes exchanging an encryption key that is used to encrypt the received data records.

33. (Previously Presented) The method of claim 30, wherein the nonce includes a random number.

34. (Previously Presented) The method of claim 30 further comprising verifying that the nonce has not previously been received in a previously received data record.

35. (Currently Amended) The method of claim 30,

wherein the received encrypted data records include ~~are encrypted by embedding~~ an indicator ~~in each of the data records~~ indicating that the data records incorporate text that has been ~~are~~ encrypted according to an encryption scheme that encrypts records without regard to any previously transmitted data records, and

further comprising determining whether the indicator is present in each received data record and, in response to determining that the indicator is not present in a received data record, processing such received data record differently than if the indicator is set.

36. (Previously Presented) The method of claim 30, wherein

establishing a communication path with a remote computer is performed using the Transmission Control Protocol, and

received the encrypted data records is performed using the User Datagram Protocol.

37. (Previously Presented) The method of claim 30, wherein the received data records are received from a proxy server that encrypts data records the proxy server received from another server.

38. (Currently Amended) A method of securely transmitting a plurality of data records to a remote computer using an unreliable communication protocol, comprising:

(1) establishing a reliable connection with the remote computer;

(2) exchanging encryption credentials with the remote computer over the reliable connection;

(3) generating a nonce for each of a plurality of data records, wherein each nonce comprises an initialization vector;

(4) for each of the plurality of data records, encrypting the data record by

using the corresponding nonce to encrypt text, ~~each of the plurality of data records~~ and

appending the encrypted text and the corresponding nonce to ~~each of the plurality of~~ data record ~~records~~; and

(5) transmitting the plurality of data records ~~encrypted in step (4)~~ to the remote computer using an unreliable communication protocol, such that the remote computer can decrypt the text in each of the plurality of ~~encrypted~~ data records using the ~~a~~ corresponding nonce extracted from each ~~encrypted~~ data record and a previously shared encryption key.

39. (Previously Presented) The method of claim 38, wherein step (3) comprises

generating a random number as each nonce.

40. (Previously Presented) The method of claim 38, wherein step (1) is performed using the Transmission Control Protocol, and wherein step (5) is performed using the User Datagram Protocol.

41. (Previously Presented) The method of claim 38, wherein step (6) is performed using an encryption key previously shared using a reliable communication protocol.

42. (Previously Presented) The method of claim 41, wherein the reliable communication protocol is the Transmission Control Protocol.

43. (Currently Amended) A method of securely transmitting a plurality of data records to a remote computer using an unreliable communication protocol, comprising:

(1) establishing a reliable connection with the remote computer;

(2) exchanging encryption credentials with the remote computer over the reliable connection;

(3) receiving a plurality of data records from the computer using an unreliable communication protocol such that each data record is encrypted by

generating a nonce ~~for each of the plurality of data records~~, wherein the ~~each~~ nonce comprises an initialization vector,

using the nonce to encrypt ~~each of the plurality of data records~~text, and

appending the encrypted text and the nonce to ~~each of the plurality of encrypted data records~~the data record; and

(4) decrypting the encrypted text in each of the plurality of encrypted data records using thea corresponding nonce extracted from each data record and a previously shared encryption key.

44. (Previously Presented) The method of claim 43, further comprising checking to determine whether each data record received from the client computer is formatted according to a secure unreliable transmission format and, if a particular record is not formatted according to a secure unreliable transmission format, bypassing the decryption using the corresponding nonce.

45. (Previously Presented) The method of claim 43, wherein each nonce includes a randomly generated number.

46. (Previously Presented) The method of claim 43, wherein step (1) is performed using Transmission Control Protocol, and wherein step (4) is performed using User Datagram Protocol.

47. (Previously Presented) The method of claim 43, wherein the previously shared encryption key previously was shared using a reliable communication protocol.

48. (Previously Presented) The method of claim 47, wherein the reliable communication protocol is Transmission Control Protocol.

49. (New) The method of claim 23, wherein encrypting the data records using the nonce includes, for each data record:

employing the incorporated nonce to create a message authentication code corresponding to the incorporated encrypted text; and

appending the message authentication code to the data record.

50. (New) The method of claim 23, wherein encrypting the data records using the nonce includes, for each data record, producing the encrypted text by employing the incorporated nonce as an initialization vector to encrypt plaintext.

51. (New) The method of claim 50, wherein encrypting the data records using the nonce further includes, for each data record:

employing the incorporated nonce to create a message authentication code corresponding

to the incorporated encrypted text; and

appending the message authentication code to the data record.

52. (New) The method of claim 30, wherein the data records have been encrypted using the nonce by, for each data record:

employing the incorporated nonce to create a message authentication code corresponding to the incorporated encrypted text; and

appending the message authentication code to the data record.

53. (New) The method of claim 30, wherein the data records have been encrypted using the nonce by, for each data record, producing the encrypted text by employing the incorporated nonce as an initialization vector to encrypt plaintext.

54. (New) The method of claim 53, wherein the data records have been encrypted using the nonce further by, for each data record:

employing the incorporated nonce to create a message authentication code corresponding to the incorporated encrypted text; and

appending the message authentication code to the data record.

55. (New) A method of securely transmitting a plurality of data records to a remote computer using an unreliable communication protocol, comprising:

(1) establishing a reliable connection with the remote computer;

(2) exchanging encryption credentials with the remote computer over the reliable connection;

(3) generating a nonce for each of a plurality of data records;

(4) for each of the plurality of data records, encrypting the data record by

encrypting text,

using the nonce to generate a message authentication code corresponding to the encrypted text, and

appending the encrypted text, the corresponding nonce and the message authentication code to the data record; and

(5) transmitting the plurality of data records to the remote computer using an unreliable communication protocol, such that the remote computer can decrypt the text in each of the plurality of data records using the corresponding nonce extracted from each data record and a previously shared encryption key.

56. (New) The method of claim 55, wherein step (3) comprises generating a random number as each nonce.

57. (New) The method of claim 55, wherein step (1) is performed using the Transmission Control Protocol, and wherein step (5) is performed using the User Datagram Protocol.

58. (New) The method of claim 55, wherein step (6) is performed using an encryption key previously shared using a reliable communication protocol.

59. (New) The method of claim 58, wherein the reliable communication protocol is the Transmission Control Protocol.

60. (New) The method of claim 55, wherein step (4) further includes using the nonce as an initialization vector to encrypt the text.

61. (New) A method of securely transmitting a plurality of data records to a remote computer using an unreliable communication protocol, comprising:

(1) establishing a reliable connection with the remote computer;

(2) exchanging encryption credentials with the remote computer over the reliable connection;

(3) receiving a plurality of data records from the computer using an unreliable communication protocol such that each data record has been encrypted by

generating a nonce,

encrypting text,

using the nonce to generate a message authentication code corresponding to the encrypted text, and

appending the encrypted text, the nonce, and the message authentication code to the data record; and

(4) decrypting the encrypted text in each of the plurality of encrypted data records using the corresponding nonce extracted from each data record and a previously shared encryption key.

62. (New) The method of claim 61, further comprising checking to determine whether each data record received from the client computer is formatted according to a secure unreliable transmission format and, if a particular record is not formatted according to a secure unreliable transmission format, bypassing the decryption using the corresponding nonce.

63. (New) The method of claim 61, wherein each nonce includes a randomly generated number.

64. (New) The method of claim 61, wherein step (1) is performed using Transmission Control Protocol, and wherein step (4) is performed using User Datagram Protocol.

65. (New) The method of claim 61, wherein the previously shared encryption key previously was shared using a reliable communication protocol.

66. (New) The method of claim 65, wherein the reliable communication protocol is Transmission Control Protocol.

67. (New) The method of claim 55, wherein each data record has been encrypted by also

using the nonce as an initialization vector to encrypt the text.